Cryptographic Key Management Workshop

Session 6:
Testing and Evaluation

March 4, 2014

Miles E. Smid

Security Assessment Overview

(Section 11)

- PA:11.1 A Federal CKMS **should** be subject to security assessments by a team of people that collectively have experience and expertise in a) Computer Security, b) Cryptography, c) Cryptographic protocols, d) distributed system design, etc., etc., etc.

Full Security Assessment
(Section 11.1)

- PR:11.1 A Federal CKMS **shall** undergo a security assessment before becoming operational and include the following:
  - A review of security testing by the CKMS developer,
  - An architectural review of the CKMS design and the FCKMS planned architecture,
  - A review of third-party testing, and
  - Functional and security testing, including conducting penetration tests

Full Security Assessment

(Section 11.1)

- PR:11.2 A Federal CKMS **shall** undergo and pass a security assessment under the following Circumstances:
  - Before initial operation,
  - After major system changes, and
  - Immediately after the occurrence or suspected occurrence of a compromise

- PR:11.3 A Federal CKMS **shall** be assessed to ensure that it supports the FCKMS security policies of its service-using organizations.

Review of Third-Party Testing and Verification
(Section 1.1.1)

- PR:11.4 During a security assessment, the assessment team **shall** verify that NIST-approved cryptographic algorithms are supported in the FCKMS and have been validated under the NIST CAVP.

- PR:11.5 During a security assessment, the assessment team **shall** verify that all cryptographic modules have been validated for conformance to FIPS 140(-2) under the NIST CMVP.

Architectural Review of System Design (Section 11.1.2)

- PR:11.6 An architectural review **shall** be conducted on a Federal CKMS prior to becoming operational.
- PR:11.7 The assessment team for a Federal CKMS **shall** have access to all CKMS design information, third-party-validation information and results of FCKMS/CKMS testing

Functional and Security Testing
(Section 11.1.3)

- PR:11.8 A Federal CKMS **shall** undergo functional and security testing, including usability tests, by the CKMS developer, FCKMS service provider, and/or a third party before initial operation.

Penetration Testing (Section 11.1.4)

- PR:11.9 Before becoming operational, a Federal CKMS **shall** be subjected to penetration testing by a team that includes individuals who did not assist in the CKMS design.

Periodic Security Review
(Section 11.2)

- PA:11.10 The security of a Federal CKMS **should** be reviewed annually to assure that it is operating with the latest security updates incorporating all current CKS implementer-supported software.

Incremental Security Assessment (Section 11.3)

- PR:11.10 A Federal CKMS **shall** undergo an incremental security assessment after any change (authorized or unauthorized) is made to any security-critical part of the FCKMS
- PR:11.11 An incremental security assessment for a Federal CKS **shall** include the identification of any changes to the system since the last security assessment, and architectural review of any design changes, and functional and security testing of the FCKMS.

Incremental Security Assessment
(Section 11.3)

- PR:11.12 A Federal CKMS **shall support producing a report following an incremental security assessment that includes the following:**
  - The reasons for any changes,
  - Inconsistencies that could have arisen between the CKMS design, the FCKMS implementation, and this Profile,
  - The results of the assessment, including all discovered security defects, and
  - Any corrective actions to be performed and the dates by which the actions must be completed.

Summary

- **Shall**
  - Full security assessment: developer review, architectural review, security testing, third-party testing, functional testing, assessment of support of FCKMS security policies, NIST approved and validated algorithms, validation of cryptographic modules, penetration testing.
  - All this shall be done before initial operation, after major system change, and after compromise.

Summary

- Shall
  - – Incremental security assessment: identification of changes, functional and security testing, reasons for changes, inconsistencies, results, corrective actions
  - – Done whenever a change is made.

Summary

- **Should**
  - Security Assessment by team of experts in many areas of security, support all needed interfaces to assess security, support security assurance tests, verify that non-cryptographic software and hardware have been validated under the Common Criteria, verify that the entire FCKMS or parts thereof have been tested and verified

Summary

- **Should**
  - Test penetration scenarios, analyze results, perform functional testing, include experts in computer security communications system design and testing, software testing, vulnerability analysis, and security threat analysis.
  - Penetration testing **should** be done every two years

Summary

- **Should**
  - Periodic security review annually for latest updates.

Open Discussion

- Does this seem reasonable?
- Is it affordable?
- Is it likely to get done?